View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

東北大学機関リポジトリ
TOUR
Tohoku University Repository

Towards a Classification of Knowledge-of-Exponent Assumptions in Cyclic Groups

著者	Kraiem Firas Alexandre
number	64
学位授与機関	Tohoku University
学位授与番号	情博第694号
URL	http://hdl.handle.net/10097/00130185

氏名	フィラス　アレクサンドル　クライエム FIRAS　ALEXANDRE　KRAIEM
学位の種類	博　士　（情報科学）
学位記番号	情　博　第６９４号
学位授与年月日	令和元年９月２５日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	Towards a Classification of Knowledge-of-Exponent Assumptions in Cyclic Groups （巡回群上のべき指数抽出仮定の分類に関する研究）
論文審査委員	（主査）東北大学教授　静谷　啓樹 東北大学教授　周　暁　東北大学教授　菅沼　拓夫 東北大学准教授　磯辺　秀司

論　文　内　容　要　旨

1 Introduction

Cryptography can be broadly defined as the design of systems, called *cryptographic systems* or *cryptographic schemes*, that are capable of maintaining their functionality in the presence of adversarial entities that attempt to make them deviate from their intended behaviour [9]. In the classical cryptographic task of *encryption*, for instance, a cryptographic system called an *encryption scheme* is used by two parties to exchange messages over a public channel in such a way as to make it impossible for any third party to obtain the contents of the exchanged messages. This property, called *privacy* or *confidentiality*, must be maintained regardless of the strategy employed by such a third party in its attempts.

A question that immediately arises when considering such schemes is how one should evaluate their "security", *i.e.*, whether and to what extent they satisfy the privacy requirement. The modern approach to this question is based on computational complexity theory and was pioneered around 1980 [5, 10, 14]. It asserts that such schemes should be considered secure if (and only if) any information about a plaintext that is contained in a corresponding ciphertext cannot be "efficiently" obtained by any third party.

However, in the current state of our knowledge in complexity theory, the security of most cryptographic systems cannot be proved in that sense unconditionally, and must be proved under the assumption that certain computational tasks are difficult (in a suitable sense). Of course, in order to increase our confidence in the security of such systems, it is necessary to increase our confidence in the validity of the assumptions under which their security is proved. Traditionally, this was done by admitting as valid the assumption that a problem is difficult when a considerable amount of research effort had been devoted to the search of efficient solutions to it without any (or much) success. (One such problem is the *integer factoring problem* [3]: given an integer, find a non-trivial factor of it.) In recent years, however, new assumptions are introduced very frequently, and, as pointed out for instance by Naor [12], it is sometimes not clear whether proving the security of a system under a new assumption is much different from simply assuming that the system is secure.

This proliferation of new assumptions raises questions both for cryptographers, who design new cryptographic systems, and for cryptanalysts, who attempt to "break" those systems by showing that the underlying assumptions are in fact false. For the former, what are the best assumptions on which to base their constructions? And for the latter, what are the best assumptions on which to focus their efforts? A solution to these dilemmas was proposed by Ghadafi and Groth in 2017 [8] for a class of assumptions which they call "target assumptions" and which includes for instance the well-known computational Diffie-Hellman (CDH) assumption [5]. Secondly, they identify a small subclass of assumptions (called "Uber-assumptions") within the large class, and show that if all the Uber-assumptions hold, then all the target assumptions hold as well.

Such a result is useful both to cryptographers and to cryptanalysts. Cryptographers can use any target assumption as the basis of their systems, and be confident that they will remain secure at least as long as none of

the Uber-assumptions is broken (since if their chosen assumption is false, then at least one Uber-assumption is false as well). Cryptanalysts, meanwhile, have a higher chance of success if they focus on the Uber-assumptions, since they give a small set of assumptions that is guaranteed to contain at least one false assumption (unless all the assumptions in the large class are true, in which case there is no hope of proving that any assumption is false anyway).

In this thesis, we attempt to apply a similar analysis to another type of assumptions, called "knowledge-of-exponent assumptions" (KEAs). Despite questions surrounding their non-falsifiability [12], KEAs have been used to construct systems for which no construction under falsifiable assumptions is known (or even possible), such as succinct non-interactive zero-knowledge protocols [11, 6]. Moreover, at least one such construction (a variant of the construction of [6, 13]) is already being used in a practical system, namely the Zcash digital currency [15]. Since such protocols require KEAs or other non-falsifiable assumptions [7], it can be expected that KEAs will become increasingly popular in the future, which makes it all the more important to have a solid understanding of them.

After reviewing some definitions and notation in Chapter 2, we discuss in Chapter 3 the q-power knowledge-of-exponent (q-PKE) family of assumptions introduced by Groth [11] and study its internal structure. We show in particular that, under a certain decisional assumption, the q-PKE family is *increasing*, *i.e.*, that $(q+1)$-PKE implies q-PKE. In Chapter 4, we introduce a class of KEAs, which we call *rational knowledge-of-exponent assumptions* (RKEAs), as a generalisation of the q-PKE family, and, as a first step towards identifying Uber-assumptions for this class, we show that it can be slightly simplified (*i.e.*, implied by a slightly smaller subclass).

2 Preliminaries

Algorithms We use the terminology and notation introduced by Abe and Fehr [1]. Unless otherwise stated, all the algorithms in this thesis take as input 1^κ, for a security parameter κ, and possibly additional inputs, and run in time polynomial in κ (this implicitly requires all inputs to have size polynomial in κ). Algorithms may be non-uniform and/or probabilistic.

To ease notation, 1^κ will often be omitted (*e.g.*, for an algorithm $\mathcal{A}$ we will often write $\mathcal{A}(x)$ instead of $\mathcal{A}(1^\kappa, x)$ to denote its execution on input x and security parameter κ). For two probabilistic algorithms $\mathcal{A}$ and $\mathcal{B}$ we denote by $\mathcal{A}||\mathcal{B}$ their joint execution on a common input and random tape, and we write $(u; v) \leftarrow (\mathcal{A}||\mathcal{B})(x)$ to say that the output of $\mathcal{A}$ on input x is assigned to u and the output of $\mathcal{B}$ on the same input x *and the same random tape* is assigned to v.

Group generators Throughout this thesis, we will define assumptions relative to a given *group generator*, as defined in [8].

Definition 2.1 (Group generators)**.** A *group generator* is a uniform probabilistic algorithm $\mathcal{G}$ which on security parameter κ outputs group parameters (G_p, g), where

- p is a prime with $|p| = \Theta(\kappa)$;
- G_p is (a description of) a (cyclic) group of order p, with canonical representations of group elements as binary strings and efficient algorithms for performing the group operation and deciding membership; and
- g is a random generator of G_p, chosen uniformly over all the generators.

As in [8], given a group G_p, a generator g, and an element $x \in \mathbf{F}_p$, we will denote by $[x]$ the element of G_p with discrete logarithm x relative to the generator g and the group operation of G_p, *i.e.*, $[x] \coloneqq g \circ g \circ \cdots \circ g$ for x terms. Thus the generator g is $[1]$ and the identity element is $[0]$. We will also denote the group operation *additively*, so that we have $[x + y] = [x] + [y]$ and $[kx] = k[x]$ (where $k[x] \coloneqq [x] + [x] + \cdots + [x]$ for k terms).

KEA1 The first knowledge-of-exponent assumption, which we call KEA1 following [2], was introduced in [4]. Roughly, it says that given a pair $([1], [\alpha])$ of elements of G_p, the only way to generate a pair $([k], [k\alpha])$ is the obvious way: pick k in some fashion, and compute $[k] = k[1]$ and $[k\alpha] = k[\alpha]$. In other words, any algorithm (adversary) which outputs such a pair must "know" k. This is formalised by saying that there must exist another algorithm, called an extractor, which, also given $([1], [\alpha])$, outputs k.

Assumption 2.2 (KEA1)**.** Let $\mathcal{G}$ be a group generator. We say that KEA1 holds (relative to $\mathcal{G}$) if for every non-uniform probabilistic algorithm $\mathcal{A}$ (the *adversary*) there is a non-uniform probabilistic algorithm $\chi_{\mathcal{A}}$ (the *extractor*) such that

$$\begin{aligned}\Pr\big[&(G_p,[1]) \leftarrow \mathcal{G}; \alpha \leftarrow \mathbf{F}_p; \sigma := (G_p,[1],[\alpha]);\\ &\big(([u],[v]);k\big) \leftarrow (\mathcal{A}||\chi_{\mathcal{A}})(\sigma) :\\ &\big([v] = \alpha[u]\big) \wedge \big([u] \neq k[1]\big)\big] \leq \text{negl}.\end{aligned}$$

3 The q-PKE family of assumptions

In this chapter we investigate the internal structure of the q-power knowledge-of-exponent (q-PKE) family of assumptions, which was introduced in [11] as a generalisation of KEA1 and other KEAs that were introduced afterwards. These assumptions are as follows.

Assumption 3.1 (q-PKE)**.** Let $\mathcal{G}$ be a group generator, and $q \in \mathbf{N}$. We say that q-PKE holds (relative to $\mathcal{G}$) if for every non-uniform probabilistic adversary $\mathcal{A}$ there is a non-uniform probabilistic extractor $\chi_{\mathcal{A}}$ such that

$$\begin{aligned}\Pr\big[&(G_p,[1]) \leftarrow \mathcal{G}; x, \alpha \leftarrow \mathbf{F}_p;\\ &\sigma := (G_p,[1],[x],\ldots,[x^q],[\alpha],[\alpha x],\ldots,[\alpha x^q]);\\ &\big(([u],[v]);(k_0,\ldots,k_q)\big) \leftarrow (\mathcal{A}||\chi_{\mathcal{A}})(\sigma) :\\ &\big([v] = \alpha[u]\big) \wedge \big([u] \neq \textstyle\sum_{i=0}^{q} k_i[x^i]\big)\big] \leq \text{negl}.\end{aligned}$$

We note that KEA1 is 0-PKE. It was shown in [2] that 1-PKE implies 0-PKE; the proof there readily extends to show that, for any q, q-PKE implies 0-PKE.

Theorem 3.2 (Generalisation of Proposition 2 from [2])**.** *Let $\mathcal{G}$ be a group generator, and $q \in \mathbf{N}$. If q-PKE holds for $\mathcal{G}$, then 0-PKE holds for $\mathcal{G}$.*

A natural question is then to ask whether this can be generalised to show that in general $(q+1)$-PKE implies q-PKE. We show that this is the case under certain circumstances, namely, when a decisional version of the Diffie-Hellman exponent assumption holds.

Assumption 3.3 (q-decisional Diffie-Hellman exponent (q-DDHE))**.** Let $\mathcal{G}$ be a group generator, $\mathcal{A}$ be a non-uniform probabilistic adversary, $q \in \mathbf{N}^*$, and $b \in \{0,1\}$, and consider the following experiment $\mathsf{Exp}^{q\text{-ddhe-}b}_{\mathcal{G},\mathcal{A}}(\kappa)$.

- $(G_p,[1]) \leftarrow \mathcal{G}; x, r \leftarrow \mathbf{F}_p$.
- If $b = 0$, then $\sigma := (G_p,[1],[x],\ldots,[x^q],[r])$; else, $\sigma := (G_p,[1],[x],\ldots,[x^q],[x^{q+1}])$.
- $b' \leftarrow \mathcal{A}(\sigma)$.
- Output b'.

We let

$$\mathsf{Adv}^{q\text{-ddhe}}_{\mathcal{G},\mathcal{A}}(\kappa) = \Big|\Pr\big[\mathsf{Exp}^{q\text{-ddhe-}1}_{\mathcal{G},\mathcal{A}}(\kappa) = 1\big] - \Pr\big[\mathsf{Exp}^{q\text{-ddhe-}0}_{\mathcal{G},\mathcal{A}}(\kappa) = 1\big]\Big|$$

be the *advantage* of $\mathcal{A}$ (in q-DDHE) relative to $\mathcal{G}$, and we say that q-DDHE holds in $\mathcal{G}$ if every adversary has negligible advantage, *i.e.*, if for every non-uniform probabilistic adversary $\mathcal{A}$, we have $\mathsf{Adv}^{q\text{-ddhe}}_{\mathcal{G},\mathcal{A}} \leq \text{negl}$.

Theorem 3.4. *Let $\mathcal{G}$ be a group generator, and $q \in \mathbf{N}^*$. If q-DDHE and $(q+1)$-PKE hold for $\mathcal{G}$, then q-PKE holds for $\mathcal{G}$.*

4 Rational KEAs (RKEAs)

In this section, we propose a definition of a large class of assumptions, with the goal of capturing not only the KEAs that have appeared in the literature thus far, but also those that are likely to appear in the future. We then show that this large class is implied by a slightly smaller subclass.

We call these assumptions *rational knowledge-of-exponent assumptions* (RKEAs), and define them as a generalisation of the q-PKE family, analogously to how target assumptions are defined in [8]. Namely, instead

of using only powers of x in the exponent, we allow arbitrary rational functions of several variables. We start by defining a very general notion of *non-interactive knowledge assumptions* (NIKAs) analogous to the non-interactive computational assumptions of [8].

Definition 4.1 (Non-interactive knowledge assumptions (NIKAs))**.** A *non-interactive knowledge assumption* consists of an instance generator $\mathcal{I}$, a verifier $\mathcal{V}$, and a knowledge verifier $\overline{\mathcal{V}}$, defined as follows.

- $(\mathsf{pub}, \mathsf{priv}) \leftarrow \mathcal{I}$: $\mathcal{I}$ is a uniform probabilistic algorithm which, on input 1^κ (where κ is a security parameter), outputs a pair of public/private information $(\mathsf{pub}, \mathsf{priv})$. We omit the input 1^κ as usual.
- $0/1 \leftarrow \mathcal{V}(\mathsf{pub}, \mathsf{priv}, \mathsf{sol})$: $\mathcal{V}$ is a uniform deterministic algorithm which, on input $(\mathsf{pub}, \mathsf{priv})$ and a purported solution sol, outputs 1 if the solution is "correct" and 0 otherwise.
- $0/1 \leftarrow \overline{\mathcal{V}}(\mathsf{pub}, \mathsf{priv}, \mathsf{sol}, \mathsf{sec})$: $\overline{\mathcal{V}}$ is a uniform deterministic algorithm which, on input $(\mathsf{pub}, \mathsf{priv}, \mathsf{sol})$ and a purported "secret" sec, outputs 1 if the secret is "correct" and 0 otherwise.

We say that the assumption holds if for any non-uniform probabilistic algorithm $\mathcal{A}$ (the *adversary*) there is a non-uniform probabilistic algorithm $\chi_{\mathcal{A}}$ (the *knowledge extractor*, or just the *extractor*) such that

$$\Pr\big[(\mathsf{pub}, \mathsf{priv}) \leftarrow \mathcal{I}; (\mathsf{sol}; \mathsf{sec}) \leftarrow (\mathcal{A} || \chi_{\mathcal{A}})(\mathsf{pub}) : \mathcal{V}(\mathsf{pub}, \mathsf{priv}, \mathsf{sol}) = 1 \wedge \overline{\mathcal{V}}(\mathsf{pub}, \mathsf{priv}, \mathsf{sol}, \mathsf{sec}) = 0\big] \leq \text{negl}.$$

Definition 4.2 (Rational knowledge-of-exponent assumptions (RKEAs))**.** Given $d, m, n \in \mathbf{N}^*$ and a group generator $\mathcal{G}$, we say that an NIKA $(\mathcal{I}, \mathcal{V}, \overline{\mathcal{V}})$ is a (d, m, n)-RKEA if there is a uniform probabilistic algorithm $\mathcal{I}^{\text{core}}$ such that $\mathcal{I}$, $\mathcal{V}$ and $\overline{\mathcal{V}}$ are of the following forms.

- $(\mathsf{pub}, \mathsf{priv}) \leftarrow \mathcal{I}$:
  - $(G_p, [1]) \leftarrow \mathcal{G}$.
  - $\left(\left\{\frac{a_i(\mathbf{X})}{b_i(\mathbf{X})}\right\}_{i=1}^n, \mathsf{pub}', \mathsf{priv}'\right) \leftarrow \mathcal{I}^{\text{core}}(G_p)$, where the a_is and b_is are polynomials in m variables and of total degree at most d.
  - $\boldsymbol{x} \leftarrow \mathbf{F}_p^m$ conditioned on $b_i(\boldsymbol{x}) \neq 0$ for all i.
  - $\alpha \leftarrow \mathbf{F}_p$.
  - $\mathsf{pub} \coloneqq \left(G_p, \left\{\left[\frac{a_i(\boldsymbol{x})}{b_i(\boldsymbol{x})}\right]\right\}_{i=1}^n, \left\{\left[\frac{\alpha \cdot a_i(\boldsymbol{x})}{b_i(\boldsymbol{x})}\right]\right\}_{i=1}^n, \left\{\frac{a_i(\mathbf{X})}{b_i(\mathbf{X})}\right\}_{i=1}^n, \mathsf{pub}'\right)$.
  - Return $\big(\mathsf{pub}, \mathsf{priv} \coloneqq ([1], \boldsymbol{x}, \alpha, \mathsf{priv}')\big)$.
- $0/1 \leftarrow \mathcal{V}\big(\mathsf{pub}, \mathsf{priv}, \mathsf{sol} = ([u], [v])\big)$: if $[v] = \alpha[u]$, return 1; else, return 0.
- $0/1 \leftarrow \overline{\mathcal{V}}\big(\mathsf{pub}, \mathsf{priv}, \mathsf{sol}, \mathsf{sec} = (k_1, \ldots, k_n)\big)$: if $\sum_{i=1}^n k_i \left[\frac{a_i(\boldsymbol{x})}{b_i(\boldsymbol{x})}\right] = [u]$, return 1; else, return 0.

Definition 4.3 (Simple RKEAs)**.** We say that an RKEA is *simple* if $b_i(\mathbf{X}) = 1$ for all $i = 1, \ldots, n$, *i.e.*, all the rational functions output by $\mathcal{I}^{\text{core}}$ are just polynomials.

Theorem 4.4. *For any (d, m, n)-RKEA $\mathsf{A} = (\mathcal{I}_\mathsf{A}, \mathcal{V}_\mathsf{A}, \overline{\mathcal{V}}_\mathsf{A})$ there is an (nd, m, n)-simple RKEA $\mathsf{B} = (\mathcal{I}_\mathsf{B}, \mathcal{V}_\mathsf{B}, \overline{\mathcal{V}}_\mathsf{B})$ such that B implies A.*

References

[1] M. Abe and S. Fehr, *Perfect NIZK with Adaptive Soundness*. S. P. Vadhan (Ed.), *TCC 2007*, *Lecture Notes in Computer Science*, vol. 4392, pp. 118–136, Springer, 2007.
doi:10.1007/978-3-540-70936-7_7

[2] M. Bellare and A. Palacio, *The Knowledge-of-Exponent Assumptions and 3-Round Zero-Knowledge Protocols*. M. Franklin (Ed.), *CRYPTO 2004*, *Lecture Notes in Computer Science*, vol. 3152, pp. 273–289, Springer, 2004.
doi:10.1007/978-3-540-28628-8_17

[3] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, second edition. Springer, New York, 2005.
doi:10.1007/0-387-28979-8

[4] I. Damgård, *Towards Practical Public Key Systems Secure Against Chosen Ciphertext Attacks*. J. Feigenbaum (Ed.), *CRYPTO '91*, *Lecture Notes in Computer Science*, vol. 576, pp. 445–456, Springer, 1992.
doi:10.1007/3-540-46766-1_36

[5] W. Diffie and M. E. Hellman, *New Directions in Cryptography. IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, IEEE, 1976.
doi:10.1109/TIT.1976.1055638

[6] R. Gennaro, C. Gentry, B. Parno, and M. Raykova, *Quadratic Span Programs and Succinct NIZKs without PCPs*. T. Johansson and P. Nguyen (Eds.), *EUROCRYPT 2013*, *Lecture Notes in Computer Science*, vol. 7881, pp. 626–645, Springer, 2013.
doi:10.1007/978-3-642-38348-9_37

[7] C. Gentry and D. Wichs, *Separating Succinct Non-Interactive Arguments From All Falsifiable Assumptions. STOC '11: Proc. of the Forty-third Annual ACM Symposium on Theory of Computing*, pp. 99–108, ACM, 2011.
doi:10.1145/1993636.1993651

[8] E. Ghadafi and J. Groth, *Towards a Classification of Non-interactive Computational Assumptions in Cyclic Groups*. T. Takagi and T. Peyrin (Eds.), *ASIACRYPT 2017*, Part II, *Lecture Notes in Computer Science*, vol. 10625, pp. 66–96, Springer, 2017.
doi:10.1007/978-3-319-70697-9_3

[9] O. Goldreich, *On the Foundations of Modern Cryptography*. B. S. Kaliski Jr. (Ed.), *CRYPTO '97*, *Lecture Notes in Computer Science*, vol. 1294, pp. 46–74, Springer, 1997.
doi:10.1007/BFB0052227

[10] S. Goldwasser and S. Micali, *Probabilistic Encryption. Journal of Computer and System Sciences*, vol. 28, no. 2, pp. 270–299, Academic Press, 1984.
doi:10.1016/0022-0000(84)90070-9

[11] J. Groth, *Short Pairing-Based Non-interactive Zero-Knowledge Arguments*. M. Abe (Ed.), *ASIACRYPT 2010*, *Lecture Notes in Computer Science*, vol. 6477, pp. 321–340, Springer, 2010.
doi:10.1007/978-3-642-17373-8_19

[12] M. Naor, *On Cryptographic Assumptions and Challenges*. D. Boneh (Ed.), *CRYPTO 2003*, *Lecture Notes in Computer Science*, vol. 2729, pp. 96–109, Springer, 2003.
doi:10.1007/978-3-540-45146-4_6

[13] B. Parno, J. Howell, C. Gentry, and M. Raykova, *Pinocchio: Nearly Practical Verifiable Computation. 2013 IEEE Symposium on Security and Privacy*, pp. 238–252, IEEE, 2013.
doi:10.1109/SP.2013.47

[14] R. L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM*, vol. 21, no. 2, pp. 120–126, ACM, 1978.
doi:10.1145/359340.359342

[15] Zerocoin Electric Coin Company, *What are zk-SNARKs?*.
https://z.cash/technology/zksnarks/ (Accessed 9 July 2019.)

論文審査結果の要旨

現代の公開鍵系の暗号方式には安全性証明が与えられている。安全性証明とは、ある問題を解くこととその暗号系を破ることが同等であることを証明することであり、これにより、その問題を解くことが困難であるとの仮定のもとで暗号系の安全性が示される。このような仮定を暗号学的仮定と呼び、様々な問題に基づくものが知られている。一般に、一つの問題についてパラメータを変化させると難しさが変化し、また一見すると異なる二つの問題が帰着関係で結ばれることがあるが、それと並行的な議論により、暗号学的仮定にも強弱や帰着関係がある。しかし、それらが具体的に解明されているものは極めて限定的であり、それゆえ未解明の仮定を不用意に使えば、安全性証明自体は正しくとも思わぬ攻撃が成立する懸念がある。

そこで著者はこの状況を改善すべく、応用上重要な暗号学的仮定の一つである「べき指数抽出仮定(KEA 仮定)」に注目し、その仮定の強さや他の仮定との関係の解明に取り組んできた。本論文は、その成果をまとめたものであり、全編 5 章からなる。

第 1 章は序論である。

第 2 章は、概念や記号の定義と説明に充てた準備の章である。

第 3 章では、KEA 仮定の拡張版である q-PKE 仮定を定義し、KEA 仮定を包含する形で q-PKE 仮定の構造の解明を目指している。ただし、q は非負整数である。ここで KEA 仮定とは、直観的には、ある問題設定において、べき指数を知らずに計算結果を出力するのは困難という仮定である。まず、KEA 仮定に関する既知の結果から、1-PKE 仮定が成立するならば 0-PKE 仮定が成立すること、すなわち 1-PKE ⇒ 0-PKE であることを注意した上で、一般の q に対して、q-PKE ⇒ 0-PKE を証明し、既知の結果を任意の自然数に拡大した。さらに、この証明の手法を使い、典型的な鍵共有方式に付随する判定問題が困難という仮定のもとで、(q+1)-PKE ⇒ q-PKE が成り立つことも証明した。これらの結果は、KEA 仮定に関する理論を深化させるものとして高く評価できる。

第 4 章では、問題設定に多変数有理関数を導入することで q-PKE 仮定をさらに拡張した RKEA 仮定を定義し、その性質の解明を試みている。そして、RKEA 仮定を構成する一部の問題に対する仮定が成立すれば RKEA 仮定全体が成立することを証明し、拡張された仮定においても帰着構造が存在することを明らかにした。これは、KEA 仮定の一般化と構造を検討する上で、興味深い結果である。

第 5 章は結論である。

以上要するに本論文は、KEA 仮定とその拡張された仮定に対し、帰着関係の解明を通じて構造を明らかにし、新しい暗号学的仮定像を与えて理論を深化させたものであり、情報基礎科学及び暗号理論の発展に寄与するところが少なくない。

よって、本論文は、博士（情報科学）の学位論文として合格と認める。